IFW
AF 3629

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPELLANTS:	Post et al.	CONFIRMATION NO. 5081
SERIAL NO.:	09/522,619	GROUP ART UNIT: 3629
FILED:	March 10, 2000	EXAMINER: Naresh Vig
TITLE:	"METHOD FOR PROTECTING A SECURITY MODULE AND ARRANGEMENT FOR THE IMPLEMENTATION OF THE METHOD"	

MAIL STOP APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPELLANTS' MAIN BRIEF ON APPEAL

S I R:

In accordance with the provisions of 37 C.F.R. §1.192, Appellants herewith submit their brief in support of the appeal of the above-referenced application.

REAL PARTY IN INTEREST:

The real party in interest is the assignee of the application, Francotyp-Postalia AG & Co, KG, a German corporation.

RELATED APPEALS AND INTERFERENCES:

There are no related appeals and no related interferences.

STATUS OF CLAIMS:

The present application was filed with claims 1-16, claims 1-9 thereof being drawn to a method for protecting a security module, and claims 10-16 drawn to a security module. In response to a restriction requirement, claims 1-9 were elected, and claims 10-16 were cancelled. Also during prosecution, claim 2 was cancelled, the subject matter thereof having been incorporated in independent claim 1.

Accordingly, claims 1 and 3-9 that are the subject of the present appeal constitute all pending claims of the application.

STATUS OF AMENDMENTS:

No Amendment was filed following the Final Rejection dated January 5, 2004.

SUMMARY OF THE INVENTION:

The method that is set forth in the claims on appeal is for assuring protection against tampering with a security module, such as a security module in a postage meter wherein monetary data are stored for use in franking postal items. In general terms, the method for protecting a security module which is the subject matter of the claims on appeal includes the steps of monitoring at least one of the status, the proper use, or the replacement of the security module using at least two function units in the security module, signaling at least one status controlled by a first of the function units, and erasing sensitive (security relevant) data with a second of the function units if an improper use or replacement is detected.

Two embodiments of an apparatus for executing the method of the claims on appeal are disclosed in the original application, respectively in Fig. 1 and Fig. 4. For explaining the method for the purpose of the present appeal, it is sufficient to rely on the embodiment of Figure 1.

Figure 1 shows a block diagram of the security module 100 with the contact groups 101, 102 for connection to an interface 8 as well as to the battery contact posts 103 and 104 of a battery interface for a battery 134. (p.11, l.7-9) Although the security module 100 is potted with a hard casting compound, the battery 134 of the security module 100 is replaceably arranged on a printed circuit board outside the casting compound. (p.11, l.9-11) The printed circuit board carries the battery contact

posts 103 and 104 for the connection of the poles of the battery 134. The security module 100 is plugged to a corresponding interface 8 of the motherboard 9 with the contact groups 101, 102. (p.11, l.11-14) The first contact group 101 has a communicative connection to the system bus of a control unit, and the second contact group 102 serves the purpose of supplying the security module 100 with the system voltage. (p.11, l.14-17) Address and data lines 117, 118 as well as control lines 115 proceed via the pins P3, P5-P19 of the contact group 101. The first contact group 101 and/or the second contact group 102 is/are fashioned for static and dynamic monitoring of the plugged state of the security module 100. (p.11, l.17-20) The supply of the security module 100 with the system voltage of the motherboard 9 is realized via the pins P23 and P25 of the contact group 102, and a dynamic and static unplugged state detection by the security module 100 is realized via the pins P1, P2 or, respectively, P4. (p.11, l.20-23)

In a known way, the security module 100 has a microprocessor 120 that contains an integrated read-only memory (internal ROM; not shown) with the specific application program that the postal authority or the respective mail carrier has approved for the postage meter machine. Alternatively, a standard read-only memory ROM or FLASH memory can be connected to the module-internal data bus 126. (p. 12, l.1-5)

In a known way, the security module 100 has a reset circuit unit 130, an application circuit (ASIC) 150 and a logic unit 160 that serves as a control signal generator for the ASIC. The reset circuit unit 130 or the application circuit 150 and the logic unit 160 as well as further memories which may be present (not shown) are

supplied with system voltage U_{s+} via the lines 191 and 129, this being supplied from the motherboard when the franking device is switched on. (p. 12, l.6-11)

Via a diode 181 and the line 136, the system voltage U_{s+} is also present at the input of the voltage monitoring unit 12. A second operating voltage U_{b+} is supplied at the output of the voltage monitoring unit 12, this being available via the line 138. When the franking device is switched off, only the battery voltage Ub+ that is available, rather than the system voltage U_{s+}. (p. 12, l.14-18) The battery contact post 104 lying at the negative pole is connected to ground. Battery voltage is supplied from the battery contact post 103 at the positive pole, to the input of the voltage monitoring unit via a line 193, via a second diode 182 and via the line 136. Alternatively to the two diodes 181, 182, a commercially available circuit can be utilized as a voltage switchover 180. (p. 12, l.8-22)

The output of the voltage monitoring unit 12 is connected via a line 138 to an input for this second operating voltage U_{b+} of the processor 120, this leading at least to a RAM memory area and guaranteeing a non-volatile storage thereat as long as the second operating voltage U_{b+} is present with the required amplitude. The processor 120 preferably contains an internal RAM 124 and a real time clock (RTC) 122 as the aforementioned RAM area. (p.13, l.1-6)

The voltage monitoring unit 12 in the security module 100 executes resettable self-holding that is interrogated by the processor 120 via a line 164 and can be reset via a line 135. For resetting the self-holding, the voltage monitoring unit 12 includes a circuit, wherein the resetting is triggered only when the battery voltage has risen above the predetermined threshold. (p.13, l.7-11)

The lines 135 and 164 are respectively connected to terminals (pin 1 and pin 2) of the processor 120. The line 164 delivers a status signal to the processor 120, and the line 135 delivers a control signal to the voltage monitoring unit 12. (p.13, l.12-14)

The line 136 at the input of the voltage monitoring unit 12 also supplies the unplugged status detection unit 13 with operating or battery voltage. (p.13, l.15-16) The unplugged status detector unit 13 emits a status signal on the line 139 terminal (pin) P5 of the processor 120, that identifies a "plugged" or "unplugged" status by its logic level. (p.13, l.16-18) The processor 120 interrogates the status of the detection unit 13 via the line 139. (p.13, l.18-19) When normal operation is restored (after an "unplugged" status) the detection unit 13 is reset by the processor 120 from terminal P4 via the line 137. (p.13, l.19-21) After being set, a static check for connection is carried out. To that end, ground potential that is present at the terminal P4 of the interface 8 of the postal security module PSM 100 is interrogated via a line 192 and can only be interrogated when the security module 100 is properly plugged in. (p.13, l.21- p.14, l.2) With the security module 100 plugged in, the terminal P23 of the interface 8 is at ground potential of the negative pole 104 of the battery 134 of the postal security module PSM 100 and thus interrogation at the terminal P4 of the interface 8 can take place by the connection unit 13 via the line 192. (p.14, l.2-5)

Monitoring as to whether the security module 100 has been unplugged is undertaken by the unplugged status detection unit 13. A voltage level is monitored at the pin 4 of the interface unit 8 via the connection to ground. (p.14, l.20-22) Given replacement of the function unit, this connection to ground is interrupted, and the unplugged status detection unit 13 registers this event as stored information. (p.14,

l.22-24) Since the storage of this information for every separation of the security module 100 from the interface unit 8 is assured by the specific, battery-operated circuit structure, an interpretation of this information can ensue at any time when a re-commissioning is desired. (p.15, l.1-4) The regular interpretation of this unplugged condition signal on the line 138 of the unplugged condition detection unit 13 makes it possible for the processor 120 to erase sensitive data without modifying the accounting and customer data in the NVRAM memories. (p.15, l.4-7) The momentary status of the postal security module with the erased, sensitive data can be interpreted as a maintenance status when replacement, repair or other similar procedures are regularly undertaken. (p.15, l.7-9) Since the sensitive data of the function unit are erased, an error due to tampering with the postal security module 100 is precluded. The sensitive data are, for example, cryptographic keys. The processor 120 - in the maintenance status - prevents a core functionality of the postal security module such as, for example, an accounting and/or calculating of a security code for the security mark in a security imprint. (p.15, l.9-14)

To be placed back into operation, the postal security module 100 is initially plugged-in and electrically connected to the corresponding interface unit 8 of a mail processing device. (p.15, l.15-17) Subsequently, the device is turned on and thus the postal security module is again supplied with system voltage U_{s+}. (p.15, l.17-18) Due to this specific status, the proper installation of the postal security module must now be re-checked by its function unit. (p.15, l.18-20) To this end, a second stage of a check (dynamic plugged condition detection) is undertaken. The error-free transmission exchange of information serves as proof of the proper installation, this exchange taking place via an operative connection setup between the first function

unit (processor 120) and the current loop 18 of the interface unit 8. This is a pre-requisite for a successful re-commissioning. (p. 15, l.20-p.16, l.2)

A re-initialization of the sensitive data is still additionally required for status change into the normal operating condition. A communication is undertaken between the postal security module 100 and a third party, such as a remote data center, which communicates the security data. After successful communication, the unplugged condition detection unit 13 is reset, and the postal security module 100 re-assumes its normal operating condition. The re-commissioning is thus completed. (p. 16, l. 3-8)

ISSUES

The following issues are presented for review:

Whether the subject matter of claims 1 and 4-9 would have been obvious to a person of ordinary skill in the field of security module design and operation under the provisions of 35 U.S.C. §103(a), based on the teachings of United States Patent No. 5,805,711 (Windel et al.) in view of the teachings of United States Patent No. 6,456,987 (Pauschinger), and further in view of a website printout entitled "Strategy and IX Products from Hughes Network Systems (hereinafter "HNS"); and

Whether the subject matter of claim 3 would have been obvious to a person of ordinary skill in the field of security module design and operation under the provisions of 35 U.S.C. §103(a) based on the teachings of Windel et al., Pauschinger, HNS, and further in view of the teachings of United States Patent No. 6,019,281(Emmett).

GROUPING OF CLAIMS:

The patentability of claims 1 and 3-9 stands or falls together.

ARGUMENT:

Appellants respectfully submit the Examiner has not established a prima facia case of obviousness under 35 U. S.C. §103(a), because the Examiner has not made any effort to identify, in the cited references, an element allegedly corresponding to the "first function unit" or an element corresponding to the "second function unit" as set forth in independent method claim 1. The method disclosed and claimed in the present application explicitly requires that at least some of the method steps be performed by one of these function units, and each of those function units is explicitly stated in claim 1 to be located in a security module. Therefore, in order to substantiate an obviousness rejection of claim 1 under 35 U.S.C. §103(a) it is necessary to locate teachings in the prior art which teach that the method steps of claim 1 are performed by these first and second function units, in the manner set forth in claim 1. Appellants respectfully submit the Examiner has not even located teachings in the prior art conforming to the basic method features of claim 1, much less teachings wherein those features are performed by first and second function units in a security module, as explicitly required in claim 1.

Moreover, Appellants submit the HSN reference has no relevancy to claim 1. That reference is primarily directed to Internet networking using various types of servers. Although the system disclosed in that reference may or may not make use of non-volatile memories (there is no explicit statement in that regard in the HSN article), there certainly is no teaching in that reference to employ a security module containing a non-volatile memory, as explicitly required in claim 1. The Examiner has stated that it is a matter of design choice as to what type of data can be stored in a non-volatile memory, however, this still does not provide any teaching regarding

the use of a non-volatile memory to store security data in a security module. Similarly, with regard to the Windel et al reference, the Examiner has stated that it is a matter of design choice to program whatever features are necessary for achieving a particular result. If these types of statements were sufficient to support a rejection under 35 U.S.C. §103(a), virtually every computer or processor arrangement would, according to the Examiner, be obvious, since they all involve a particular selection of programmed features and a particular selection of memory contents. If, as the Examiner has proposed, both of these selections are merely "design choices," then it is difficult to envision any type of computer or processor wherein such "design choices" are not made. It is incumbent on the Examiner to identify specific citations to the references relied upon by the Examiner wherein teachings for a specific programmed feature or a specific stored memory item can be found, otherwise the Examiner is simply proposing an obviousness rejection based on what is within the capabilities of a person of ordinary skill in the art, or what would be "obvious to try." The United States Court of Appeals for the Federal Circuit in many decisions has stated that neither of these is the proper standard for assessing non-obviousness under 35 U.S.C. §103(a).

The Federal Circuit stated in *In re Lee* 227 F.3d 1338, 61 U.S.P.Q. 2d 1430 (Fed. Cir. 2002):

> "The factual inquiry whether to combine references must be thorough and searching. ...It must be based on objective evidence of record. This precedent has been reinforced in myriad decisions, and cannot be dispensed with."

Similarly, quoting C.R. Bard, Inc. the M3 Systems, Inc. 157 F.3d 1340, 1352, 48 U.S.P.Q. 2d 1225, 1232 (Fed. Cir. 1998), the Federal Circuit in *Brown &*

Williamson Tobacco Court v. Philip Morris, Inc., 229 F.3d 1120, 1124-1125, 56 U.S.P.Q. 2d 1456, 1459 (Fed. Cir. 2000) stated:

> [A] showing of a suggestion, teaching or motivation to combine the prior art references is an 'essential component of an obviousness holding'.

In *In re Dembiczak,* 175 F.3d 994,999, 50 U.S.P.Q. 2d 1614, 1617 (Fed. Cir. 1999) the Federal Circuit stated:

> Our case law makes clear that the best defense against the subtle but powerful attraction of a hindsight-based obviousness analysis is rigorous application of the requirement for a showing of the teaching or motivation to combine prior art references.

Consistently, in *In re Rouffet,* 149 F.3d 1350, 1359, 47 U.S.P.Q. 2d 1453, 1459 (Fed. Cir. 1998), the Federal Circuit stated:

> [E]ven when the level of skill in the art is high, the Board must identify specifically the principle, known to one of ordinary skill in the art, that suggests the claimed combination. In other words, the Board must explain the reasons one of ordinary skill in the art would have been motivated to select the references and to combine them to render the claimed invention obvious.

In *Winner International Royalty Corp. v. Wang,* 200 F.3d 1340, 1348-1349, 53 U.S.P.Q. 2d 1580, 1586 (Fed. Cir. 2000), the Federal Circuit stated:

> Although a reference need not expressly teach that the disclosure contained therein should be combined with another, ... the showing of combinability, in whatever form, must nevertheless be clear and particular.

Lastly, in *Crown Operations International, Ltd. v. Solutia, Inc.,* 289 F.3d 1367, 1376, 62 U.S.P.Q. 2d 1917 (Fed. Cir. 2002), the Federal Circuit stated:

> There must be a teaching or suggestion within the prior art, within the nature of the problem to be solved, or within the general knowledge of

a person of ordinary skill in the field of the invention, to look to particular sources, to select particular elements, and to combine them as combined by the inventor.

Moreover, with regard to the Windel et al reference, the Examiner has acknowledged that Windel et al does not disclose monitoring proper insertion of a security module. This is not surprising, because the apparatus disclosed in the Windel et al reference does not have a security module. The Windel et al reference makes use of secured data, protected by means of a security key, as schematically indicated in Figure 8 thereof, but does not have a security module in which such data or such a key are stored. The security key, as indicated in Figure 8, is merely contained in an internal OTP-ROM. Simply because a memory may happen to have security data stored therein does not mean that the memory then becomes a "security module." Particularly in the field of postage meters, a "security module" has a well understood meaning, and it is the module in which monetary data are stored, i.e. the electronic credit for use in franking, and therefore it is protected from tampering not only by electronic protection but also by mechanical protection. Appellants recognize that claim 1 uses only the term "security module," and does not explicitly describe the type of data stored therein, however, such a level of detail is not necessary to distinguish the method steps of claim 1 over the teachings of the Windel et al reference, even as modified by the secondary references.

Appellants respectfully submit it is hindsight in the extreme to propose modifying a reference which does not even contain a security module so as to include the step of monitoring a security module. Certainly no teachings in that regard are provided in any manner whatsoever by the HSN article, which the

Examiner has apparently relied on as a teaching to modify the Windel et al reference in this regard.

The Examiner noted that the Windel et al patent makes reference to United States Patent No. 4,812,985 as teaching the use of sensors within a postage meter machine for detecting manipulative activity (tampering), so as to set a flag in appropriate memories. Although this may be an accurate description of the teachings of United States Patent No. 4,812,965, there is no teaching in the Windel et al reference as to how or whether such a technique could be incorporated in the apparatus disclosed and claimed in the Windel et al patent. The Examiner appears to believe that simply because a reference contains a statement regarding a particular reference, it would have been obvious to incorporate whatever is contained in that statement into the apparatus disclosed in the reference. Clearly, the provisions of 35 U.S.C. §103(a) require more than simply a listing of disjointed and unconnected statements regarding the teachings of various prior art references. Some linking teaching, motivation or inducement must be cited by the Examiner in order to properly substantiate a rejection under Section 103(a), and the Examiner has provided no linking teaching whatsoever with regard to the Windel et al reference, or United States Patent No. 4,812,965 discussed therein, or the HSN article.

As to re-initialization, the Examiner relied on a similar statement in the Pauschinger reference, regarding a teaching in another patent (United States Patent No. 5,590,198) to employ a removable meter insert which requires a user password for operating the franking system, and which can also be operated with a super password generated by a data center. Again, this is merely a statement of a

particular teaching of a particular prior art reference and the Examiner has not provided persuasive argument as to how this individual teaching could be incorporated in the Windel et al system, particularly in view of the fact that there is no security module in the Windel et al apparatus. Moreover, the re-initialization which is described in the Pauschinger reference, in the context of United States Patent No. 5,590,198, provides no teaching with regard to the operation or interaction of first and second function units, as set forth in claim 1 of the application. The statement cited by the Examiner merely informs a person of ordinary skill in the art that re-initialization can be accomplished by contacting a data center, or, if an appropriate super password is present, re-initialization can take place without contacting the data center. How this re-initialization takes place (i.e. whether it is by the interaction of first and second function units as set forth in claim 1) is nowhere disclosed or discussed in the Pauschinger reference.

Claim 1 explicitly makes clear that, as part of the monitoring of proper insertion, the second function unit detects a status indicating at least one of improper use and improper replacement of the security module and that the second function unit continues to monitor this status to determine its continued existence. If and when this status ceases to exist, the first function unit then initiates the re-initialization, and, in the last step of claim 1, after the re-initializing, the first and second function units are enabled to re-commission the security module. No such method steps are disclosed or suggested in the references relied upon by the Examiner. Even if some features of claim 1 may be conceptually described in the references separately and individually, there is no teaching in any of the references

that those separately and individually described method steps should be performed by first and second function units, as explicitly required in claim 1.

Claim 1, therefore, would not have been obvious to a person of ordinary skill in the art based on the teachings of Windel et al, Pauschinger and the HSN article. Claims 4-9 add further steps to the non-obvious method of claim 1, and therefore would not have been obvious to a person of ordinary skill in the art under 35 U.S.C. §103(a), based on the references cited by the Examiner, for the same reasons discussed above in connection with claim 1.

As to claim 3, that claim incorporates the subject matter of claim 1 therein, and therefore even if the Examiner is completely correct with regard to his characterizations of the teachings of the Emmett et al reference, the basic Windel et al/Pauschinger/HSN combination does not teach the subject matter of claim 1, and therefore even if that combination were modified in accordance with the teachings of Emmett et al, a method as set forth in claim 3 still would not result. Claim 3, therefore, would not have been obvious to a person of ordinary skill in the art based on the teachings of the references cited by the Examiner.

CONCLUSION:

For the foregoing reasons, Appellants submit the Examiner is in error in law and in fact in rejecting claims 1 and 3-9. Reversal of these rejections is therefore justified, and the same is respectfully requested.

This Appeal Brief is accompanied by a check for the requisite fee in the amount of $330.00.

Submitted by,

Steven H. Noll (Reg. 28,982)

SCHIFF, HARDIN LLP
CUSTOMER NO. 26574
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606
Telephone: 312/258-5790
Attorneys for Appellants.

CERTIFICATE OF MAILING

I hereby certify that an original and two copies of this correspondence are being deposited with the United States Postal Service as First Class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on June 1, 2004.

Steven H. Noll

STEVEN H. NOLL

APPENDIX "A"

1. (Currently Amended) A method for protecting a security module comprising the steps of:

storing security relevant data in a non-volatile memory of a security module and inserting said security module in a device motherboard;

monitoring proper insertion of said security module on said device motherboard with a first function unit and a second function unit in said security module;

signaling at least one security-related status of said security module with said first function unit;

in said monitoring of proper insertion, detecting a status indicating at least one of improper use and improper replacement of said security module with said second function unit and, upon a detection of said status indicating at least one of said improper use and said improper replacement, said second function unit causing said security-relevant data to be erased;

in said monitoring of proper insertion, monitoring a continued existence of said status with said second function unit and detecting, with said second function unit, when said status no longer exists;

when said second function unit detects that said status no longer exists, initiating re-initializing, with said first function unit, any erased, security-relevant data; and

after said re-initializing, enabling each of said first function unit and said second function unit to re-commission said security module.

3. A method as claimed in claim 1 comprising the additional steps of:

normally operating said security module with system voltage from a device containing said device motherboard and, in an absence of said system voltage, operating said security module with a battery; and

monitoring a status of said battery with said second function unit as a basis for detecting at least one of said improper use and said improper replacement.

4. A method as claimed in claim 1 comprising providing a third function unit and inhibiting said security module with said third function unit during at least one of replacement of said security module on said device motherboard and damage to said security module.

5. A method as claimed in claim 4 comprising detecting said damage to said security module with said third function unit.

6. A method as claimed in claim 1 comprising evaluating a running time credit with said first function unit and, upon expiration of said time credit, signaling a suspicious status of said security module with said first function unit.

7. A method as claimed in claim 6 comprising the additional steps of:

after expiration of said time credit, said first function unit establishing a communication with a remote data source; and

restoring normal operation to said security module via said communication.

8. A method as claimed in claim 6 comprising selecting a duration of said time credit to obtain a time credit of selected duration, and loading said time credit of selected duration into a memory in said security module, said memory being accessible by said first function unit.

9. A method as claimed in claim 6 wherein said time credit is a first time credit, and comprising the additional steps of monitoring a second time credit with said first function unit, which is longer than said first time credit, and signaling a status designating a device containing said device motherboard as being inoperable when said second time credit expires.

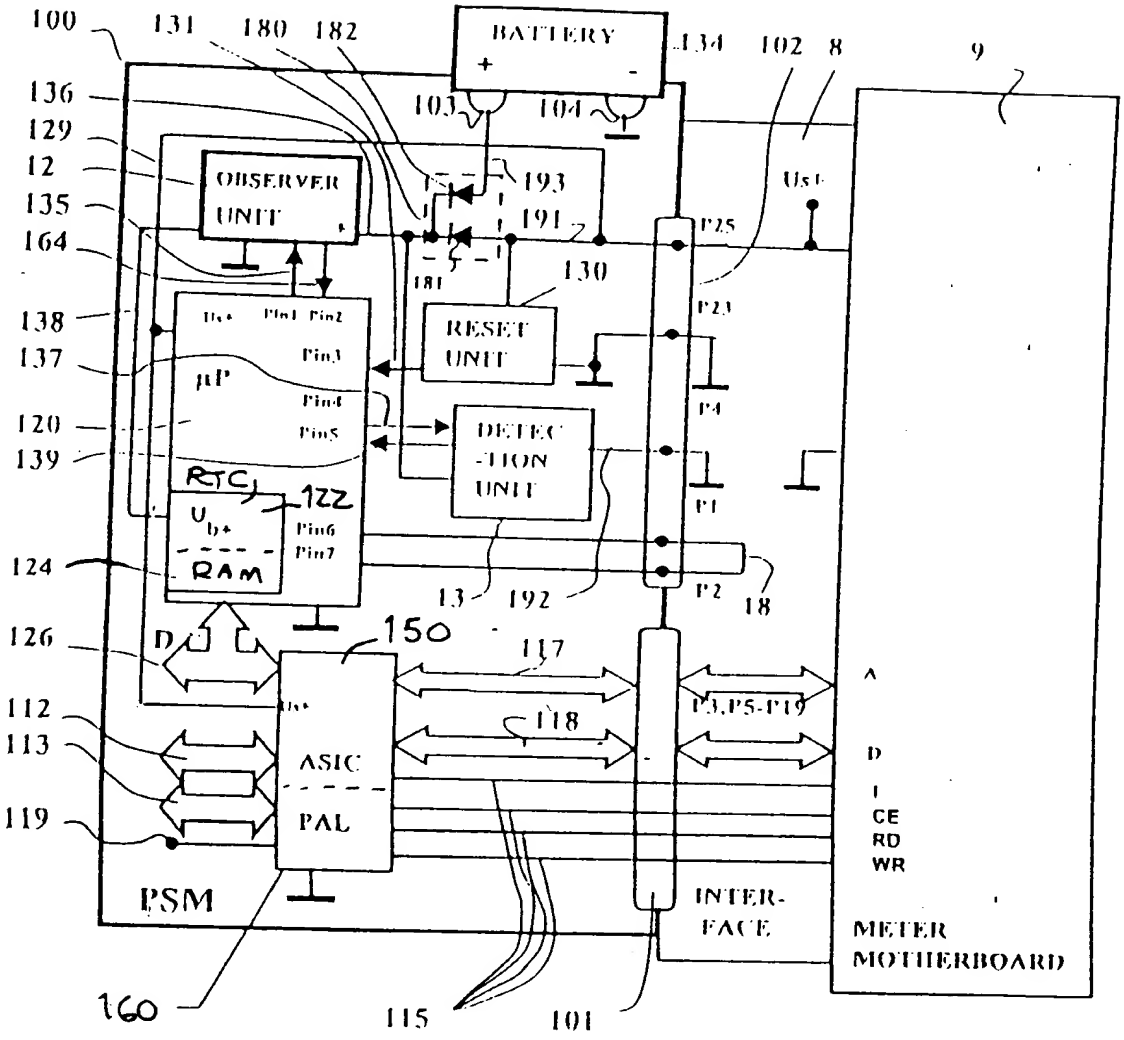
100
131
180
182
BATTERY
134
102
8
9
136
129
12
135
164
103
104
OBSERVER UNIT
193
191
181
130
RESET UNIT
P25
P23
P4
P1
P2
18
138
137
120
139
μP
Pin1
Pin2
Pin3
Pin4
Pin5
DETEC-TION UNIT
RTC
122
Ub+
Pin6
Pin7
RAM
124
13
192
126
D
150
117
112
113
119
ASIC
PAL
118
P3,P5-P19
A
D
I
CE
RD
WR
PSM
INTER-FACE
METER MOTHERBOARD
160
115
101

Fig. 1